Using Malware Analysis to Improve Security Requirements on Future Systems

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Nancy R. Mead
August 25, 2014

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN “AS-IS” BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

DM-0001544

Topics

Problem Statement

Creation of Malware-Analysis Driven Use Cases

A case study in support of Malware-Analysis Driven Use Cases

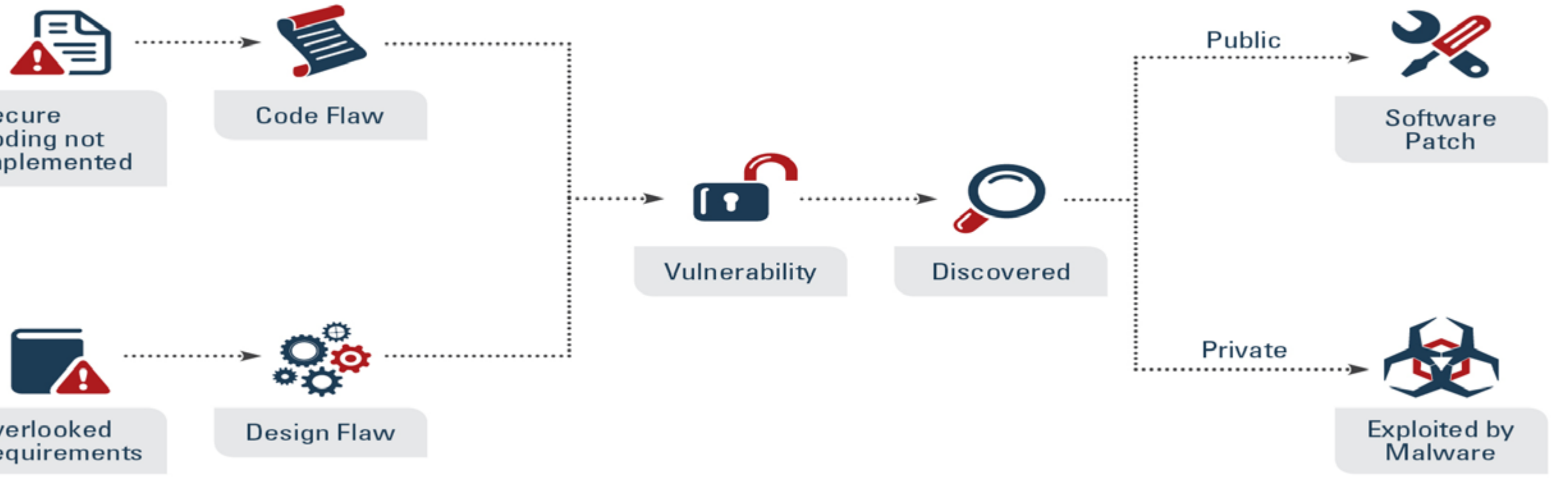
Discussion

Problem Statement

Despite the reported attacks on critical systems, operational techniques such as malware analysis are not used to inform early lifecycle activities, such as security requirements engineering

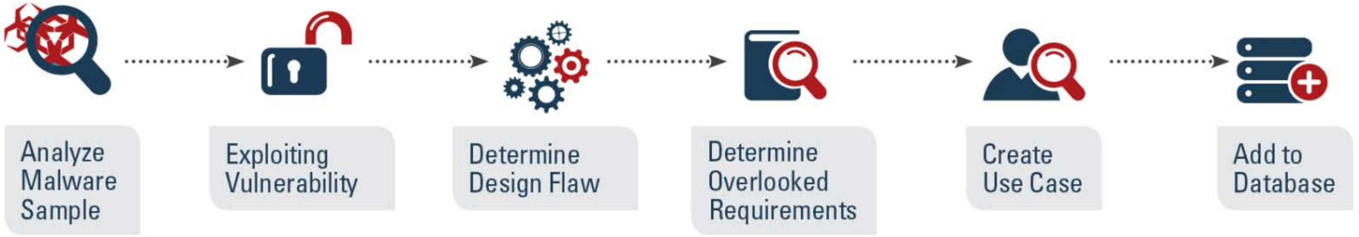
- Operational techniques like malware analysis are typically used for patch generation – they don’t usually get fed back into the development process.
- Developers of security requirements tend to either start with a blank slate or with large databases of candidate requirements and use cases.
- Creation and prioritization of security requirements may be done without the insights gained from analysis of prior attacks, especially those that are specific to a particular domain.

Creation of a Vulnerability



- Code flaws result from lack of secure coding
- Design flaws result from overlooked requirements
- Unknown amount of time needed to discover a vulnerability
  - Discovered in software
  - Discovered as part of a malware exploit
- If Discovered:
  - and made public → Patch it!
  - and kept private → Exploit it!

Malware-analysis Driven Use Case Creation



Malware already analyzed by domain expert

- We start process with the analysis results

It's exploiting a vulnerability!

- Get the exploit details

Design or Code Flaw?

If Design, what requirements were overlooked that led to this flaw?

Create a use case from those requirements and add to DB

- Goal: requirements should prevent this flaw from occurring again

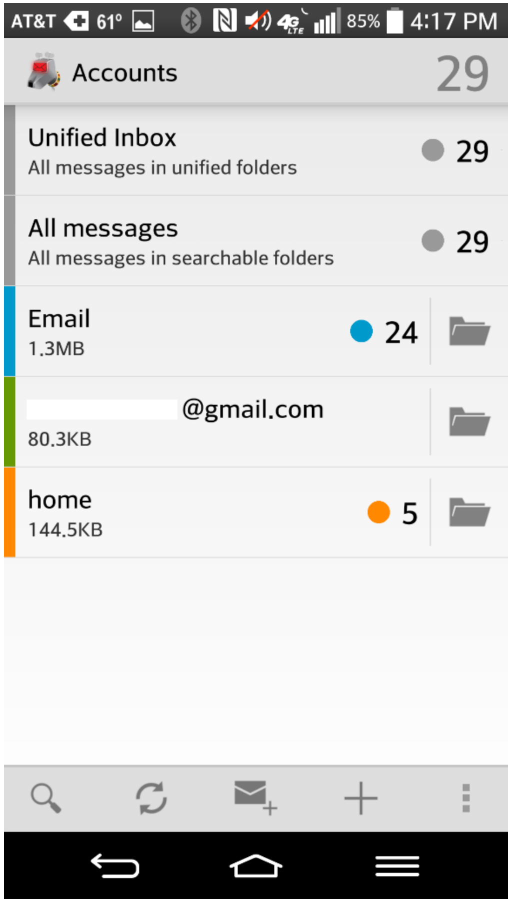
Process for Creating Use Cases

1. Obtain the results from completed static and dynamic analysis of a malicious code sample.
2. Analyses reveal the malware is exploiting a vulnerability from either a code flaw or a design flaw.
3. In the case of a design flaw, the exploitation scenario corresponds to a misuse case that should be described.
4. The misuse case is analyzed to determine the overlooked security requirement and its corresponding use case.
5. The security requirements statement and corresponding use case are added to a requirements database.
6. The requirements database is used in future software development projects. (Traceability is retained across the steps and usage of requirements from the database is tracked).

Case Study - Application

K-9 Mail Application for Android

- Open Source
- Compatible with IMAP, POP3, and Exchange 2003/2007
- Provides searching and other common smartphone email client functionality.
- User expectation of privacy and security.



AT&T 61° 85% 4:17 PM

Accounts 29

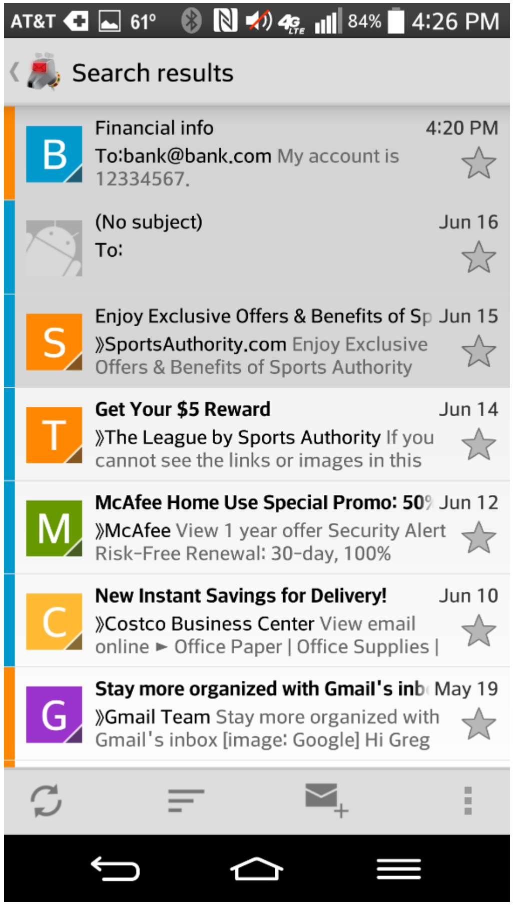
Unified Inbox
All messages in unified folders ● 29

All messages
All messages in searchable folders ● 29

Email
1.3MB ● 24

[redacted]@gmail.com
80.3KB

home
144.5KB ● 5



AT&T 61° 84% 4:26 PM

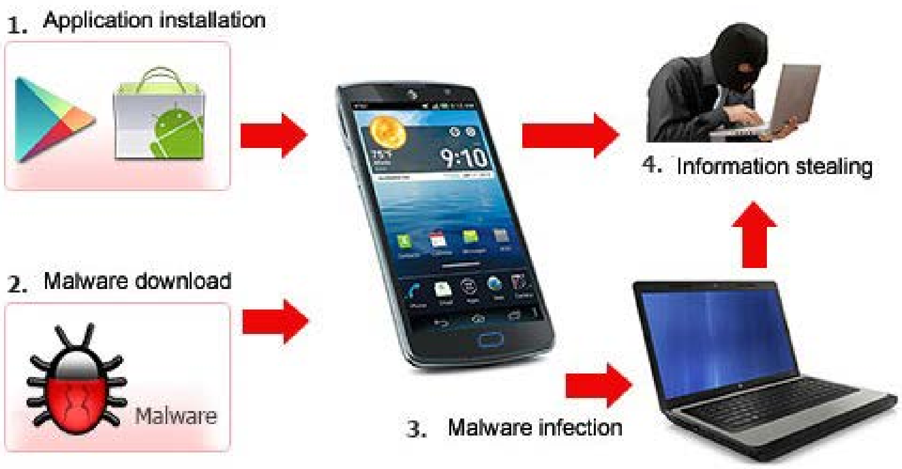
Search results

B	Financial info To:bank@bank.com My account is 12334567.	4:20 PM
	(No subject) To:	Jun 16
S	Enjoy Exclusive Offers & Benefits of Sp »SportsAuthority.com Enjoy Exclusive Offers & Benefits of Sports Authority	Jun 15
T	Get Your $5 Reward »The League by Sports Authority If you cannot see the links or images in this	Jun 14
M	McAfee Home Use Special Promo: 50% »McAfee View 1 year offer Security Alert Risk-Free Renewal: 30-day, 100%	Jun 12
C	New Instant Savings for Delivery! »Costco Business Center View email online ► Office Paper | Office Supplies |	Jun 10
G	Stay more organized with Gmail's inb »Gmail Team Stay more organized with Gmail's inbox [image: Google] Hi Greg	May 19

Case Study - Vulnerability

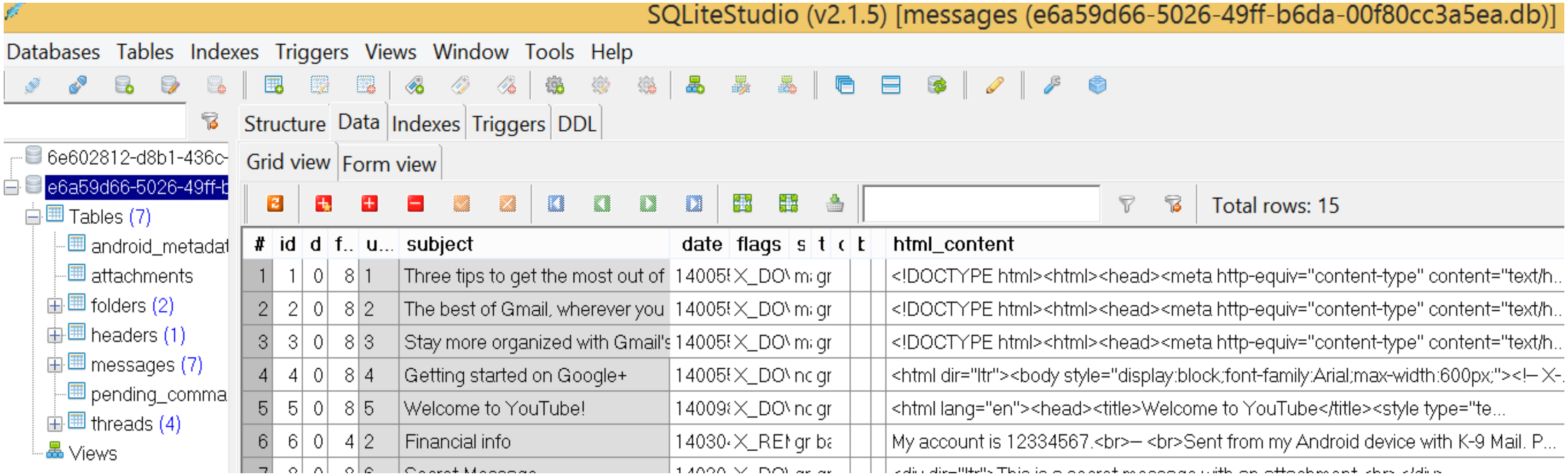
DroidCleaner

- Trojan malware
  - Claims to perform an Android tune-up.
  - Sends premium rate SMS messages.
  - Uploads data from the Android External Storage area to hacker's servers.



Case Study – Exploitation Scenario

- Trojan
  - Social Engineering to trick user into installing DroidCleaner:
    - Install software
    - Grant access to external storage, internet access
- K-9 Mail configured to store email in External Storage
- DroidCleaner uploads External Storage to hacker server.
- Hacker examines contents. Email contents disclosed:



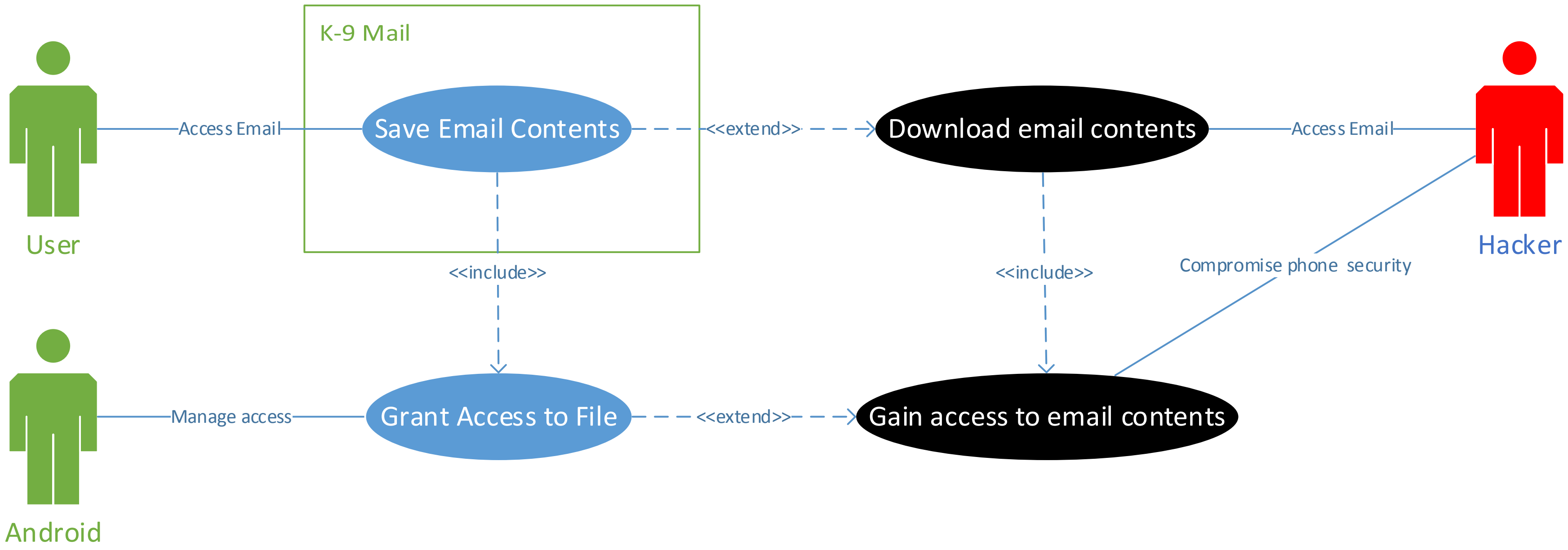
SQLiteStudio (v2.1.5) [messages (e6a59d66-5026-49ff-b6da-00f80cc3a5ea.db)]

Total rows: 15

#	id	d	f..	u...	subject	date	flags	s	t	(	t		html_content
1	1	0	8	1	Three tips to get the most out of	14005!	X_DO\	m:	gr				<!DOCTYPE html><html><head><meta http-equiv="content-type" content="text/h..
2	2	0	8	2	The best of Gmail, wherever you	14005!	X_DO\	m:	gr				<!DOCTYPE html><html><head><meta http-equiv="content-type" content="text/h..
3	3	0	8	3	Stay more organized with Gmail's	14005!	X_DO\	m:	gr				<!DOCTYPE html><html><head><meta http-equiv="content-type" content="text/h..
4	4	0	8	4	Getting started on Google+	14005!	X_DO\	nc	gr				<html dir="ltr"><body style="display:block;font-family:Arial;max-width:600px;"><!– X-.
5	5	0	8	5	Welcome to YouTube!	14009!	X_DO\	nc	gr				<html lang="en"><head><title>Welcome to YouTube</title><style type="te...
6	6	0	4	2	Financial info	14030·	X_RE!	gr	ba				My account is 12334567. – Sent from my Android device with K-9 Mail. P...
7	8	0	8	6	Secret Message	14030	X_DO\	gr	gr				<div dir="ltr">This is a secret message with an attachment. </div>

Case Study – Misuse Case

Gain Access to Email Contents



Case Study – New Requirement

Requirement Number: 1	
Requirement	1.1 Email contents shall be protected from unauthorized access. Email contents shall be stored in an area only available to the application (Android Internal Storage default configuration) – and/or – protected through encryption which cannot be decrypted using data available in Android External Storage. 1.2 Processes with access to External Storage shall not have the ability to view K-9 Mail contents in clear text. If external storage is selected, a warning message or mitigation, such as encryption is recommended.
Category	Data Protection
Priority	High
Cost	Medium
Misuse Case	MUC2
Rationale	Due to the high risk of data theft malware on Android, it is not safe to assume data kept on the phone is private, therefore the email contents must be kept in a form which cannot be read even if the Hacker has access to the storage location.

Discussion

Do specific types of malware exist that are likely to occur in specific kinds of critical systems, such as control systems?

Does the 6-step process make sense?

Does malware analysis help to identify new requirements for such systems?

Does malware analysis help to prioritize requirements for such systems?

Acknowledgements

Jose Morales, CERT – co-authored the paper

Greg Alice, Boeing – contributed the case study

Contact Information

Nancy R. Mead
Fellow and Principal Researcher
CERT
Email: nrm@sei.cmu.edu

Web
www.sei.cmu.edu
www.sei.cmu.edu/contact.cfm

U.S. Mail
Software Engineering Institute
Customer Relations
4500 Fifth Avenue
Pittsburgh, PA 15213-2612
USA

Customer Relations
Email: info@sei.cmu.edu

Telephone:	+1 412-268-5800
SEI Phone:	+1 412-268-5800
SEI Fax:	+1 412-268-6257